4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/810,927	03/25/2004	Carl E. Banzhof	4121-37300	1914

30652 7590 05/02/2007

CONLEY ROSE, P.C.
5700 GRANITE PARKWAY, SUITE 330
PLANO, TX 75024

EXAMINER	
COLIN, CARL G	
ART UNIT	**PAPER NUMBER**
2136	

MAIL DATE	DELIVERY MODE
05/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/810,927	BANZHOF ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 February 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,5,7,8,10,11,13,14,18-25,30 and 32-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,5,7,8,10,11,13,14,18-25,30 and 32-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *see att*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 2/22/2007, applicant has amended claims 1, 5, 7, 8, 10, 11, 13, 14, 18, 21-25, 30, cancels claims 2-4, 6, 9, 12, 15-17, 26-29, and 31; and adds claims 32-45. The following claims 1, 5, 7-8, 10-11, 13-14, 18-25, 30, and 32-45 are presented for examination.

1.1 In response to communications filed on 2/22/2007, the objection to claims 22-29 have been withdrawn with respect to the amendment.

2. Applicant's arguments, pages 23-28, filed on 2/22/2007, with respect to the rejection of the claims have been fully considered, but they are moot in view of a new ground of rejection. Applicant's arguments regarding Dadhia are not persuasive. Applicant argues that Dahdia discloses the computers already connected to the network and have already accessed the network. Examiner respectfully disagrees. Paragraph 18 of Dadhia cites,

> "The dynamic protection system may use a firewall installed on the user computer system to restrict access of the instances of the application to resources. A user computer that is not connected to a local area network also may use the dynamic protection system. The dynamic protection system identifies the security level of that instance of the application and places limitations on its execution as appropriate. For example, the protection system may configure the firewall so that the instance of the application cannot access the Internet."

Applicant has amended to more particularly point out the claimed invention. Upon further consideration, a new ground of rejection is set forth below.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 3/13/2007 was filed after the mailing date of the Non-Final Rejection on 12/15/2006. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 5, and 38-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication 2005/0188419 to **Dadhia et al** in view of US Patent Publication 2005/0138433 to **Linetsky**.

As per claim 1, **Dadhia et al** substantially discloses a method for protecting a computer network from vulnerabilities, comprising: *quarantining* (isolating by placing a limitation on the

instance of the application of a computer system) a computer system from said computer network by said computer system raising a firewall resident on the computer system whenever physically connecting or reconnecting said computer system until said quarantined computer system is remediated, (see page 4, claims 2 and 3) (see page 3, paragraph 25) wherein said quarantine of said computer system is self-initiated, and wherein said firewall allows specified permitted communications while blocking all other communications (see page 3, paragraph 25). **Dadhia et al** discloses the dynamic protection system establishes limitations through actions of rules when the instance of the application first attempts to access a network resource after startup, or when the computer system connects to the network (see page 4, claims 2 and 3). As interpreted by the Examiner, access a network resource after startup is a physical connection or reconnection to the network, therefore, the isolation is performed whenever said computer system disconnects from and subsequently reconnects to said computer network. **Dadhia et al** discloses that the dynamic protection system may use a firewall installed on the user computer system to restrict access of the instances of the application to resources (see page 2, paragraph 18) and the firewall may be configured to access only to a resource that will allow it to update to a more recent security level (see page 3, paragraph 25) which meets the recitation of raising a firewall resident on the computer system whenever physically connecting or reconnecting said computer system until said quarantined computer system is remediated, wherein said firewall allows specified permitted communications while blocking all other communications; the filter rules are explained in more details in paragraph 19. **Dadhia et al** discloses determining if the computer system requires remediation, wherein the determination is performed by a component of the computer network communicating with the computer system, and wherein the

communication between the computer system and the component is one of the specified permitted communications (see page 2, paragraph 18 and page 3, paragraph 25); remediating the computer system using information from the component of the computer network in accordance with the determination (see page 3, paragraph 25 and page 2, paragraph 17, lines 11-16); **Dadhia et al** discloses upon completing remediation of said quarantined computer system, the computer system lowering the firewall to allow all communication between the computer system and the computer network (see pages 1-2, paragraph 12). Although not using the same language, it has been shown that **Dadhia et al** discloses the inventive features of claim 1 as claimed. For purpose of clarity, **Linetsky** in an analogous art discloses quarantining and limiting access to a computer system whenever the computer system physically connecting or reconnecting said computer system (see page 8, paragraph 75 and page 5, paragraph 52) because this will prevent security breaches from physical connection and reconnection and will ensure that connected devices are trusted all the time. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to isolate said computer system whenever physically connecting or reconnecting said computer system as suggested by **Linetsky**. One of ordinary skill in the art would have recognized some of the advantages suggested by **Dadhia et al** for incorporating a protection system with a firewall to allow specific permitted communication while blocking others and would have recognized some of the advantages suggested by **Linetsky** for the importance of maintaining a safe environment by making a device untrusted upon connection, disconnection, and reconnection of the device (see **Dadhia et al,** page 2, paragraph 18 and **Linetsky,** page 5, paragraphs 52 and 55).

As per claim 5, **Dadhia et al** discloses a specified permitted communication between the computer system and the component of the network includes a flow of vulnerability resolution (see page 2, paragraph 12).

As per claim 38, **Dadhia et al** discloses wherein determining if the computer system requires remediation includes determining if the computer system has any pending remediations (patch not yet installed) (see paragraph 12).

As per claim 39, **Dadhia et al** discloses wherein a specified permitted communication between the computer system and the component of the network includes information needed for the computer system and the computer network to confirm that the computer system is attempting to re-enter its home network (see paragraph 18).

As per claim 40, **Dadhia et al** discloses wherein a specified permitted communication between the computer system and the component of the network includes information identifying the computer system and the component of the network (see paragraph 18 and claim 13).

5. **Claims 7, 8, 10, 11, 13, 21-23, 41-43** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication 2005/0188419 to **Dadhia et al** in view of US Patent Publication 2005/0138433 to **Linetsky** in view of US Patent Publication 2003/0208606 to **Maguire et al**.

As per claim 7, **Dadhia et al** substantially discloses *for a computer network comprised of a plurality of computer systems and a client remediation server coupled to each one of said plurality of computer systems, said client remediation server remediating said computer network by resolving vulnerabilities in said plurality of computer systems, a method for protecting said remediated computer network from unresolved vulnerabilities, comprising:* if one of said computer systems of said remediated computer network is physically disconnected from said remediated computer network, upon a subsequent physical re-connection of said computer system to said remediated computer network (see page 4, claims 2 and 3), said computer system raising a firewall resident on the computer system to temporarily limiting exchanges between said remediated computer network and said computer systems until said computer system has been verified by said remediation server (see page 2, paragraph 18 and pages 1-2, paragraph 12), wherein said computer system lowers the firewall upon said remediation server verifying said computer system (see page 3, paragraph 25 and page 2, paragraph 17, lines 11-16). As interpreted by the Examiner, access a network resource after startup is a physical connection or reconnection to the network, therefore, the isolation is performed whenever said computer system disconnects from and subsequently reconnects to said computer network. **Dadhia et al** discloses that the dynamic protection system may use a firewall installed on the user computer system to restrict access of the instances of the application to resources (see page 2, paragraph 18) and the firewall may be configured to access only to a resource that will allow it to update to a more recent security level (see page 3, paragraph 25) which meets the recitation of raising a firewall resident on the computer system whenever physically connecting or reconnecting said computer system until said quarantined computer system is remediated, wherein said firewall

allows specified permitted communications while blocking all other communications; the filter rules are explained in more details in paragraph 19. **Dadhia et al** discloses upon completing remediation of said quarantined computer system, the computer system lowering the firewall to allow all communication between the computer system and the computer network (see pages 1-2, paragraph 12). Although not using the same language, it has been shown that **Dadhia et al** discloses the inventive features of claim 1 as claimed. For purpose of clarity, **Linetsky** in an analogous art discloses quarantining and limiting access to a computer system whenever the computer system physically connecting or reconnecting said computer system (see page 8, paragraph 75 and page 5, paragraph 52) because this will prevent security breaches from physical connection and reconnection and will ensure that connected devices are trusted all the time. **Linetsky** suggests that the invention is not limited to one type of device connected to a computer (see page 5, paragraph 52). To show that a peripheral device may be interpreted as a computer system connected to a network, **Maguire et al** in an analogous art discloses selectively isolating a computerized device from a network and discloses peripheral devices as (servers, computers, terminals, workstations, input devices, etc.) (see page 2, paragraphs 22 and 25). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to isolate said computer system whenever physically disconnecting or reconnecting said computer system as suggested above. One of ordinary skill in the art would have recognized some of the advantages suggested by **Dadhia et al** for incorporating a protection system with a firewall to allow specific permitted communication while blocking others and would have recognized some of the advantages suggested by **Linetsky** for the importance of maintaining a safe environment by making a device untrusted upon connection, disconnection,

and reconnection of the device (see **Dadhia et al,** page 2, paragraph 18 and **Linetsky,** page 5, paragraphs 52 and 55).

As per claim 8, **Dadhia et al** discloses the verification includes checking for pending remediations for said computer system (see page 3, paragraph 25).

As per claim 10, **Dadhia et al** discloses filtering access to only a remediation resource that meets the claimed limitation of limiting exchanges between said remediated computer network and said computer system includes filtering out non-remediation-related traffic (see page 3, paragraph 25).

As per claim 11, **Dadhia et al** discloses verifying said computer system includes filtering access to only a remediation resource that meets the claimed limitation of wherein verifying said computer system includes said client remediation server executing said pending remediations for said computer system (see page 3, paragraph 25).

As per claim 13, **Dadhia et al** discloses allowing communications and Internet access once the condition is satisfied that meets the recitation of lowering the firewall permits non-remediation-related traffic to pass between said computer system and said remediated computer network without filtering (see page 3, paragraphs 24 and 25).

As per claim 21, **Dadhia et al** substantially discloses a remediated computer network comprising: a computer system; and a client remediation server coupled to said computer system (see page 2, paragraph 18), said client remediation server configured to resolve vulnerabilities in said computer system whenever said computer system physically connects or reconnects to said computer network (see page 4, claims 2 and 3, and page 2, paragraph 18); and further discloses the computer system cannot access the Internet and restricting the instance access until a patch to a vulnerability that has been exploited by a worm has been installed (see paragraph 12) that meets the recitation of wherein said computer system includes a firewall for isolating said computer system from said remediated computer network upon said computer system physically connecting or reconnecting to said computer network, until said client remediation server resolves vulnerabilities of said computer system (see page 2, paragraph 18 and pages 1-2, paragraph 12). **Dadhia et al** discloses that the dynamic protection system may use a firewall installed on the user computer system to restrict access of the instances of the application to resources (see page 2, paragraph 18) and the firewall may be configured to access only to a resource that will allow it to update to a more recent security level (see page 3, paragraph 25) wherein said computer system includes a firewall for isolating said computer system from said remediated computer network upon said computer system physically connecting or reconnecting said computer system until said client remediation server resolves vulnerabilities of said computer system. Although not using the same language, it has been shown that **Dadhia et al** discloses the inventive features of claim 1 as claimed. For purpose of clarity, **Linetsky** in an analogous art discloses quarantining and limiting access to a computer system whenever the computer system physically connecting or reconnecting said computer system (see page 8,

paragraph 75 and page 5, paragraph 52) because this will prevent security breaches from physical connection and reconnection and will ensure that connected devices are trusted all the time. **Linetsky** suggests that the invention is not limited to one type of device connected to a computer (see page 5, paragraph 52). To show that a peripheral device may be interpreted as a computer system connected to a network, **Maguire et al** in an analogous art discloses selectively isolating a computerized device from a network and discloses peripheral devices as (servers, computers, terminals, workstations, input devices, etc.) (see page 2, paragraphs 22 and 25). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to isolate said computer system whenever physically disconnecting or reconnecting said computer system as suggested above. One of ordinary skill in the art would have recognized some of the advantages suggested by **Dadhia et al** for incorporating a protection system with a firewall to allow specific permitted communication while blocking others and would have recognized some of the advantages suggested by **Linetsky** for the importance of maintaining a safe environment by making a device untrusted upon connection, disconnection, and reconnection of the device (see **Dadhia et al,** page 2, paragraph 18 and **Linetsky,** page 5, paragraphs 52 and 55).

As per claim 22, the combined references disclose the claimed computer network of claim 21. **Dadhia et al** discloses a computer system access a network resource after startup that meets the recitation of disconnecting and reconnecting from the network (see page 4, claims 2-3) and discloses the dynamic protection system establishes limitations through actions of rules when an instance of an application first executing (see page 2, paragraph 14) or first attempts to

access a network resource after startup (see page 4, claim 2), that meets the recitation of *wherein said computer system is configured to raise said firewall to isolate said computer system from said remediated computer network whenever said computer system disconnects from and subsequently reconnects to said computer network;* the filter rules are explained in more details in paragraph 19. Claim 22 is also rejected on the same rationale as the rejection of claim 21.

As per claim 23, the combined references disclose the claimed computer network of claim 22. **Dadhia et al** discloses *wherein said computer system is configured to raise said firewall upon each power-up thereof* (see page 4, claims 2-3).

As per claim 41, **Dadhia et al** discloses wherein limiting exchanges between said remediated computer network and said computer system includes allowing traffic needed for the computer system and the computer network to confirm that the computer system is attempting to re-enter its home network and allowing other remediation related traffic between the client remediation server and the computer system (see paragraph 18 and claim 13 and page 4, claims 2-3).

As per claim 42, **Dadhia et al** discloses wherein limiting exchanges between said remediated computer network and said computer system includes allowing traffic needed to identify the computer system and the client remediation server and allowing other remediation related traffic between the client remediation server and the computer system (see paragraph 18 and claim 13 and page 4, claims 2-3).

As per claim 43, the combined references disclose wherein the initiation of the connection is responsive to a physical communication link being connected between said computer system and said computer network subsequent to the communication link being disconnected (see **Linetsky,** page 5, paragraph 52). Claim 43 is rejected on the same rationale as the rejection of claim 21.

6. **Claims 24-25** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication 2005/0188419 to **Dadhia et al** in view of US Patent Publication 2005/0138433 to **Linetsky** in view of US Patent Publication 2003/0208606 to **Maguire et al**. and further in view of US Patent 5,987,611 to **Freund** *(Applicant's disclosure)*.

As per claims 24-25, the combined references disclose the claimed computer network of claim 21. **Dadhia et al** further discloses the *computer system is configured to raise said firewall upon initiating registration with a LAN* (see paragraph 18). **Dadhia et al** discloses that the invention may be implemented with the Internet, LAN, WAN, network handheld or laptop devices *(wireless devices)* attached to the network, (see paragraphs 20-21) that meets the recitation of *wherein said computer system is configured to raise said firewall upon initiating registration with said WAN.* As interpreted by the Examiner, upon accessing the network or first installation of a patch includes initiating registration since the network has to be accessed to perform registration. **Freund** in an analogous art discloses a client-based filter application *(firewall)* for monitoring whether client process has access to the Internet otherwise the

remediation for any violated rule is performed (see column 4, lines 29-33 and lines 54-63); and further discloses monitoring specific web sites and login for limiting computer access to a network or the Internet and limiting what applications can do on the Internet (see column 24, lines 1-15; column 25, lines 1-12; and column 28, lines 2-32). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to *raise said firewall upon initiating registration with said LAN or WAN.* One of ordinary skill in the art would have recognized some of advantages suggested by **Freund** so as to minimize risks within corporate LAN or other WAN accesses from client machines by regulating kinds of exchanges permissible between one computing environment and the external network or WAN including the Internet as suggested by **Freund** (see column 3, lines 35-48).

7. **Claims 14, 18-20, 44-45** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication 2005/0188419 to **Dadhia et al**.

As per claim 14, **Dadhia et al** substantially discloses *a method for protecting a computer network from nefarious software associated with a computer system being connected to said computer network, comprising: upon initiating a connection between said computer system and said computer network,* said computer system quarantining itself from said computer network by raising a firewall resident on said computer system, (see page 4, claims 2 and 3), wherein the firewall allows specified permitted communications and blocks all other communications with said computer network (see page 2, paragraph 18 and pages 1-2, paragraph 12); performing a scan on said computer system with information from a component of said computer network (see

page 1, paragraph 12); and lifting said quarantine lowering the firewall upon detected by said scan of said computer system by said computer system completing removal of any nefarious software (see pages 1-2, paragraph 12). **Dadhia et al** discloses that the dynamic protection system may use a firewall installed on the user computer system to restrict access of the instances of the application to resources (see page 2, paragraph 18) and the firewall may be configured to access only to a resource that will allow it to update to a more recent security level (see page 3, paragraph 25) which meets the recitation of *upon initiating a connection between said computer system and said computer network,* said computer system quarantining itself from said computer network by raising a firewall resident on said computer system. Although **Dadhia et al** is directed to update patches there is suggestion that the patches are used to remove vulnerabilities such as worm or virus (see page 1, paragraphs 4-5), it is apparent to one of ordinary skill in the art that an antivirus scanner with the latest patches would have the tool necessary the remove the virus when found. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the feature of removing the virus as part of the scanning process of **Dadhia et al** "to avoid risks like spreading viruses" as suggesting by **Dadhia et al** (see page 1, par. 4-5).

As per claim 18, **Dadhia et al** discloses wherein traffic between said computer system and said component of said computer network is related to said nefarious software detection and removal and is a specified permitted communication allowed to pass throuqh the firewall (see page 1, paragraphs 4, 5, and 18). Claim 18 is also rejected on the same rationale as the rejection of claim 14 above.

As per claim 19, **Dadhia et al** discloses wherein said nefarious software is a computer virus (see page 1, paragraphs 4 and 12).

As per claim 20, **Dadhia et al** discloses wherein said nefarious software is a computer virus (see page 1, paragraphs 4 and 12).

As per claim 44, **Dadhia et al** discloses wherein said quarantine of said computer system is lifted upon said component of said computer network further completing an execution of any pending remediations for said computer system (see pages 1-2, paragraphs 12-13).

As per claim 45, **Dadhia et al** discloses once the condition has been satisfied the action is performed and does not need to check any other rules that meets the recitation of wherein lowering the firewall generally permits all traffic to pass between said computer system and said remediated computer network without filtering by the firewall (see page 2, paragraph 13).

8. **Claim 30, 32-33** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication 2005/0188419 to **Dadhia et al** in view of US Patent 5,987,611 to **Freund** *(Applicant's disclosure)*.

As per claim 30, **Dadhia et al** substantially discloses *a computer system, comprising:* processor, memory, that meets the recitation of *a processor subsystem; a memory subsystem*

coupled to said processor subsystem (see paragraph 20)*; at least one application* (instance of an application or operating system) *residing in said memory subsystem and executable by said processor subsystem* (see paragraph 18); *and a firewall switchable between a closed position in which traffic to and/or from said computer system is restricted and an open position in which traffic to and/or from said computer system is unrestricted* (see paragraph 18)*; wherein said firewall is configured to switch into said closed position upon power-up of said computer system and upon initiation of registration with a computer network* (see page 4, claim 2). As interpreted by the Examiner a firewall can be active/inactive or enabled/disabled, or turned on/off that meets the recitation of switchable firewall with closed/open position as claimed. **Dadhia et al** discloses that the firewall may be configured to restrict access to only resources that will allow it to update (see paragraph. 25) and the dynamic protection system applies filtering rules to the application upon startup *(upon power-up)* and access *(upon initiation of registration)* to the network. Although not using the same terms, **Dadhia et al** disclosure reads into the claimed invention and it would have been obvious to one of ordinary skill in the art at the time the invention was made to configure the firewall to limit access to resources (page 2, lines 1-7) upon startup *(upon power-up)* of the computer system and access *(upon initiation of registration)* to the network (see page 4, claim 2) because it would ensure that the application is up-to-date as soon as the application is started and a vulnerability is not exploited as suggested by **Dadhia et al** (see page 2, paragraph 14). **Dadhia et al** discloses that the firewall may be configured to restrict access only to resources that will allow it to update the patches *(remediation server)* (see par. 25 and paragraph 12) that meets the recitation of wherein all traffic to and from said computer system is generally restricted when said firewall is switched to said closed position,

and where said firewall permits specific access through said firewall including at least to locate and communicate with a remediation server of said computer network when said firewall is switched to said closed position; and further discloses restricting access until the patched is installed (see paragraphs 12-13) that meets the recitation of wherein the firewall is configured to switch from said closed position to said open position only upon said remediation server verifying that said computer system meets standards of said network.

Freund in an analogous art discloses a client-based filter application *(firewall)* for blocking clients that have not been verified by the supervisor application and monitoring whether client process has access to the Internet otherwise the remediation for any violated rule is performed (see column 4, lines 1-4, 29-33, and lines 54-63); and further discloses monitoring specific web sites and login for limiting computer access to a network or the Internet and limiting what applications can do on the Internet (see column 24, lines 1-15; column 25, lines 1-12; and column 28, lines 2-32). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to *raise said firewall upon initiating registration with said LAN or WAN.* One of ordinary skill in the art would have recognized some of advantages suggested by **Freund** so as to minimize risks within corporate LAN or other WAN accesses from client machines by regulating kinds of exchanges permissible between one computing environment and the external network or WAN including the Internet as suggested by **Freund** (see column 3, lines 35-48).

As per claim 32, the combined references disclose the claimed computer system of claim 30. **Dadhia et al** discloses wherein the specific access through the firewall to locate and

communicate with said remediation server of said computer network is the only specific access permitted through said firewall when said firewall is switched to said closed position (see paragraph 25).

As per claim 33, the combined references disclose the claimed computer system of claim 30. **Dadhia et al** discloses verifying said computer system includes filtering access to only a remediation resource that will allow it to update to a more recent security level or redirect to another computer to configure a firewall that meets the claimed limitation of wherein communication with said remediation server includes traffic for executing pending remediations and traffic for executing supplementary remediations determined necessary by said client remediation server (see page 3, paragraphs 19 and 25).

9. **Claim 34** is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication 2005/0188419 to **Dadhia et al** in view of US Patent 5,987,611 to **Freund** *(Applicant's disclosure)* and further in view of US Patent Publication 2005/0138433 to **Linetsky** and US Patent Publication 2003/0208606 to **Maguire et al**.

As per claim 34, **Dadhia et al** substantially discloses the dynamic protection system applies filtering rules to the application upon startup (*upon power-up)* and access (*upon initiation of registration)* to the network. Although not using the same terms, **Dadhia et al** disclosure reads into the claimed invention (see paragraph 25). **Linetsky** in an analogous art discloses quarantining and limiting access to a computer system whenever the computer system physically

connecting or reconnecting said computer system (see page 8, paragraph 75 and page 5, paragraph 52) because this will prevent security breaches from physical connection and reconnection and will ensure that connected devices are trusted all the time. **Linetsky** discloses performing appropriate login and authentication upon physically connecting (see page 5, paragraph 53). **Linetsky** suggests that the invention is not limited to one type of device connected to a computer (see page 5, paragraph 52). To show that a peripheral device may be interpreted as a computer system connected to a network, **Maguire et al** in an analogous art discloses selectively isolating a computerized device from a network and discloses peripheral devices as (servers, computers, terminals, workstations, input devices, etc.) (see page 2, paragraphs 22 and 25). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to initiate registration with said computer network upon physically connecting said computer system with said computer network as suggested above so as to maintain a safe environment and making sure that the computer or user has access privileges. One of ordinary skill in the art would have recognized some of the advantages suggested by **Dadhia et al** for incorporating a protection system with a firewall to allow specific permitted communication while blocking others and would have recognized some of the advantages suggested by **Linetsky** for the importance of maintaining a safe environment by making a device untrusted upon connection, disconnection, and reconnection of the device (see **Dadhia et al,** page 2, paragraph 18 and **Linetsky,** page 5, paragraphs 52 and 55).

10. **Claims 35-37** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication 2005/0188419 to **Dadhia et al** in view of US Patent Publication 2005/0138433 to **Linetsky** and further in view of US Patent Publication 2003/0208606 to **Maguire et al**.

As per claim 35, the combined references disclose the claimed method of claim 1. **Linetsky** discloses quarantining and limiting access to a computer system whenever the computer system physically connecting or reconnecting said computer system upon power up or power down (see page 8, paragraph 75 and page 5, paragraphs 52-53) because this will prevent security breaches from physical connection and reconnection and will ensure that connected devices are trusted all the time that meets the claimed limitation of wherein physically reconnecting the computer system to the computer network includes one of detaching a physical communication link between the computer system and the computer network and subsequently attaching the physical communication link or powering down the computer system while maintaining the physical communication link and subsequently powering up the computer system. **Linetsky** suggests that the invention is not limited to one type of device connected to a computer (see page 5, paragraph 52). To show that a peripheral device may be interpreted as a computer system connected to a network, **Maguire et al** in an analogous art discloses selectively isolating a computerized device from a network and discloses peripheral devices as (servers, computers, terminals, workstations, input devices, etc.) (see page 2, paragraphs 22 and 25). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to initiate registration with said computer network upon physically connecting said computer system with said computer network as suggested above so as to maintain a safe

environment and making sure that the computer or user has access privileges. One of ordinary skill in the art would have recognized some of the advantages suggested by **Dadhia et al** for incorporating a protection system with a firewall to allow specific permitted communication while blocking others and would have recognized some of the advantages suggested by **Linetsky** for the importance of maintaining a safe environment by making a device untrusted upon connection, disconnection, and reconnection of the device (see **Dadhia et al,** page 2, paragraph 18 and **Linetsky,** page 5, paragraphs 52 and 55).

As per claim 36, the combined references disclose the claimed method of claim 35. **Linetsky** discloses performing appropriate login and authentication upon physically connecting and reconnected (see page 5, paragraph 53) that meets the recitation of wherein remediating the computer system includes performing supplemental remediations if the physical communication link is detached and subsequently attached (see paragraphs 52-53). Claim 36 is rejected on the same rationale as the rejection of claim 35.

As per claim 37, the references as combined above disclose the claimed method of claim 1. but are silent about the remediation is a "scheduled" remediation. Examiner takes official notice that scheduled patch update for instance is well known in the art and would have been an obvious modification to one of ordinary skill in the art to modify the method as combined above to include performing remediations scheduled for the computer system subsequent to the computer system disconnecting from the computer network so as to perform automatic update without relying upon the user or an administrator.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

11.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carl Colin
Patent Examiner
April 29, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

4/30/07